FILED ENTERED
LODGED RECEIVED
JUN 27 2019
AT GREENBELT
CLERK U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY DEPUTY

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF THE **APPLE ICLOUD ACCOUNT, RECORDS, AND INFORMATION** ASSOCIATED WITH THE EMAIL ADDRESSES: **HONEEFASHIONS@ICLOUD.COM, GREATLOVE88@ICLOUD.COM, HONEEY178@AOL.COM, AND EUNIQLA@YAHOO.COM,** THAT ARE STORED AT PREMISES CONTROLLED BY APPLE, INC.

Case No. 19-1836 TJS

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, August Merker, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple, Inc. ("Apple") to disclose to the government the Apple iCloud account, records, and other information, including the contents of communications, associated with the email addresses **honeefashions@iCloud.com, GREATlove88@iCloud.com, Honeey178@aol.com,** and **Euniqla@yahoo.com** (hereinafter referred to as the "TARGET ACCOUNTS"), that are stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, California. The information to be disclosed by Apple and searched by the government is described below and in Attachments A and B.

2. I am a Special Agent with the Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and have been so employed since May 2003. I am assigned to the Office of the Special Agent in Charge,

Baltimore, Maryland. I have prepared and executed numerous state and federal search warrants and assisted with Title III court-authorized intercepts. Further, I have gathered evidence of violations of both state and federal laws, interviewed numerous suspects, witnesses and informants, and have participated in the execution of search and arrest warrants in connection with the aforementioned investigations. I am currently assigned to the Counter-Proliferation Investigations Task Force, where I am responsible for conducting criminal investigations involving the illegal exportation of goods and services from the United States as well as associated money laundering violations in the District of Maryland. Prior to my appointment with HSI, I served five years as a Police Officer in Montgomery County, Maryland.

3. The facts set forth in this affidavit are based upon my personal knowledge and knowledge obtained during my participation in this investigation, including my review of documents related to this investigation, communication with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. This affidavit does not contain all of the information known to me regarding this investigation. I have included in this affidavit facts that I believe are sufficient to support a probable cause finding for the issuance of the requested warrant, but I do not purport to include each and every matter of fact observed or known to me or other law enforcement agents involved in this investigation.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. §§ 1349 (Conspiracy to Commit Mail and Wire Fraud), 1341 (Mail Fraud), 1343 (Wire Fraud), 1956 (Money Laundering Conspiracy and Money

Laundering), 2314 (Interstate Transportation of Stolen Property), and 1028A (Aggravated Identity Theft), as described in Attachment B.

PROBABLE CAUSE

A. Fraud Scheme Perpetuated by Drunz Organization.

5. Beginning in approximately December 2016, law enforcement began investigating a scheme that involved numerous coconspirators engaged in large-scale mail fraud to obtain goods sent to various points throughout the United States. To perpetuate the fraud scheme, the organization used falsified U.S. military email accounts (i.e., Daniel.Drunz@navy-mil.us) and contracting documents to obtain products such as high-end consumer products and export-controlled military communications equipment. This equipment included approximately $6.3 million in LG televisions, at least $3.2 million in sensitive export-controlled communications equipment and approximately $1.1 million dollars in iPhones and iPads. Beginning in or about October 2016, the above email account was used to defraud three companies, one in Virginia (hereinafter "Company A") and one in Maryland (hereinafter "Company B") and one headquartered in the State of Washington (hereinafter "Company C"). Company B is a Cleared Defense Contractor who develops and produces highly sensitive export-controlled communications equipment for the United States government, and Company C is a distributor of mobile devices and wireless data services, including Apple iPhones and iPads. The investigation revealed that the items procured from these companies were sent to an office space located in Chantilly, Virginia and a warehouse located in Frederick, Maryland, both leased using stolen identities and then ultimately shipped to the area of Los Angeles, California.

6. On or about August 31, 2016, Company A, that distributes LG televisions and equipment, received an email regarding a business opportunity with an individual who identified

himself as Daniel DRUNZ ("DRUNZ"). DRUNZ stated that he was a U.S. Navy contracting officer and sought to purchase 1,596 LG OLED television/monitor units from Company A, using what appeared to be electronic copies of official U.S. Navy procurement and acquisition documents containing contract number N66001-16-D-0178. On or about October 12, 2016, Company A received via email what appeared to be a U.S. Navy contract from DRUNZ for over 2,000 LG OLED television/monitor units to be delivered to what DRUNZ claimed was a warehouse owned by the U.S. Navy and located in, Chantilly, Virginia 20151, in exchange for over $7.1 million.

7. Subsequent investigation has shown that the order placed by DRUNZ was fraudulent. Records searches for DRUNZ revealed that there has never been a U.S. Navy employee named Daniel DRUNZ. A search of Department of Defense databases revealed that contract number N66001-16-D-0178 never existed. Checks with the management company show that the office located in, Chantilly, Virginia, was not rented by the U.S. Navy but instead was rented by an individual fitting the description of Janet STURMER, a co-conspirator and member of the organization, who identified herself as with the company "Paes Enterprises." On or about October 31, 2016, November 1, 2016, and November 8, 2016, numerous tractor-trailers arrived at the Chantilly, Virginia office, to deliver over 2,000 LG Electronics televisions/monitors valued at over $6,3 million. According to witnesses, crews of workers met the tractor-trailers and off-loaded the televisions/monitors into the storefront during the day. These witnesses also recounted that subsequently, the televisions/monitors were loaded into U-Haul and Budget Rental trucks that were then driven away from the Chantilly, VA office location.

8. After delivering the LG televisions/monitors, Company A attempted to receive payment from the U.S. Navy for the televisions/monitors. Company A sent a request for payment

to the Defense Finance and Accounting Service ("DFAS"), an agency of the Department of Defense ("DOD") that provides payment to DOD contractors and vendors. DFAS notified Company A on or about December 29, 2016 that the contract DRUNZ had provided was not a valid U.S. Navy contract. To date, Company A has not received any payment from DRUNZ for the televisions/monitors.

9. On or about December 5, 2016, law enforcement met with Company B. During this meeting, representatives from Company B informed law enforcement that Company B had been contacted by an individual using the name DRUNZ in or about August 2016.

10. DRUNZ contacted Company B using the email address Daniel.Drunz@navy-mil.us and identified himself as a U.S. Navy contracting official. Beginning in or about August 2016, DRUNZ provided Company B with documents that DRUNZ represented were a U.S. Navy contract bearing contract number N65236-16-D-0093. This contract called for Company B to sell DRUNZ highly sensitive communications interception equipment listed on the United States Munitions List ("USML") and therefore controlled for export under the International Trafficking in Arms Regulations ("ITAR"). Specifically, according to Company B, many of these commodities are controlled under the USML Category XI. Multiple items that were acquired by this criminal organization via the fraud scheme are so highly restricted that, according to Company B, even a photograph of the item is considered controlled under the ITAR as their existence is not public knowledge.

11. The "Ship to Address" provided to Company B by DRUNZ on the contract was the same office in Chantilly, Virginia, which DRUNZ represented to be a U.S. Navy facility. On or about October 27, 2016, Company B sent the products listed in the contract provided by DRUNZ, which were valued at approximately $3.2 million, to the final delivery address located in Chantilly,

Virginia.

12. On or about August 2, 2017, law enforcement met with Company C, during this meeting, representatives from Company C informed law enforcement that Company C had been contacted by an individual using the name DRUNZ in or about October 2016.

13. Company C received via email what appeared to be a U.S. Navy purchase order from DRUNZ for approximately 150-200 iPhones and iPads units to be delivered to what DRUNZ claimed was a facility owned by the U.S. Navy and located in Frederick, Maryland.

14. Approximately one month after the initial purchase order, DRUNZ contacted Company C and submitted an order from approximately 1,000 more iPhones to be delivered to the Frederick, Maryland address. The total value of devices shipped from Company C to the Frederick, Maryland address was over $1.1 million.

15. Records searches for DRUNZ revealed that there has never been a U.S. Navy employee named Daniel DRUNZ. A search of DOD databases revealed that the purchase order to Company C did not exist. Company C has received no payment for the items it shipped pursuant to the purchase orders provided by DRUNZ.

16. On or about February 9, 2017, a search warrant was executed at the residence of Janet STURMER. During the execution of the search warrant, law enforcement recovered several of the fraudulently obtained LG televisions from the garage and living room of the residence. STURMER stated that she had a friend named Khalid RAZAQ. RAZAQ had a friend in Nigeria who asked RAZAQ to receive a large number of televisions. STURMER stated that RAZAQ's Nigerian friend was named "Peter" (later identified as Peter UNAKALU). UNAKALU or an individual known only as MAYOR were behind the "computer work" that was done to obtain the items from Company A, Company B, and Company C. STURMER stated that RAZAQ and

UNAKALU met in prison and that UNAKALU had been deported from the United States. STURMER stated that she shipped approximately 100 of the televisions to California via UPS and approximately 50 of the televisions to California via FedEx. STURMER was also aware of heavy military computer equipment being delivered to the Chantilly, VA office space and stated that she had rented another facility in Frederick, Maryland for the purpose of receiving iPhones and laptops. STURMER said that she and RAZAQ traveled to California in September of 2016 and met with an individual named "Brandon", who lives in California (later identified as Brandon ROSS). She stated that RAZAQ and UNAKALU knew ROSS.

B. Prior Cellular Communications and Electronic Device Search Warrant Results.

17. On March 20, 2017, NKONGHO flew from Havana, Cuba to Miami, Florida. Customs and Border Protection ("CBP") officers inspected NKONGHO on her way into the United States. NKONGHO had multiple devices seized pursuant to a border search to include a cellphone. On March 29, 2017, law enforcement obtained a federal search warrant from U.S. District Court for the District of Maryland granting the examination of these devices by law enforcement (Case Number TMD 17-0941).

18. During the examination of the cellphone, law enforcement confirmed the familial relationship between NKONGHO and Peter UNAKALU, namely that they were husband and wife. Additionally, law enforcement discovered multiple conversations between NKONGHO and UNAKALU discussing the transfer of money between NKONGHO and Khalid RAZAQ for the payment and further facilitation of the fraud scheme. For example, on or about November 14, 2016, UNAKALU contacted NKONGHO and directed her to send RAZAQ $5,000 so that he can "ship product." During this conversation, UNAKALU sent RAZAQ a picture of the bank account information for RAZAQ and indicated that this bank was where NKONGHO was to transfer the

money. Shortly after, NKONGHO responded to UNAKALU by sending a picture of the bank confirmation showing the money has been transferred. These communications occurred over the WhatsApp messaging service.

19. On September 17, 2017, NJOKU, the alleged distributor of the fraudulently acquired property, flew from China to California. CBP Officers inspected NJOKU upon entry into the United States and seized multiple devices to include a cellphone pursuant to a border search. On November 9, 2017, law enforcement obtained a federal search warrant from the United States District Court for the District of Maryland granting the examination of these devices by law enforcement (Case Number TMD 17-3082).

20. Within NKONGHO's cellphone, law enforcement reviewed numerous conversations between NKONGHO and NJOKU, which revealed a close relationship not only between the NKONGHO and NJOKU but also between NJOKU and UNAKALU. Multiple conversations between NKONGHO and NJOKU further indicated a business relationship between NJOKU and UNAKALU. The communications between NKONGHO and NJOKU revealed that NKONGHO acted on behalf of UNAKALU in the United States. Of note, UNAKALU cannot travel to the United States due his prior deportations for both immigration and criminal fraud violations (U.S. District Court for the District of Delaware, Crim. No. 92-55-1). The above-noted communications occurred over WhatsApp messaging service.

21. On multiple occasions from approximately July 2015 through July 2018, as evidenced from the review of the above cellphone conversations, NJOKU sent messages via WhatsApp to NKONGHO requesting that she notify UNAKALU that he needed to contact NJOKU. On or about February 18, 2017, NKONGHO contacted NJOKU via WhatsApp and stated: "Good Morning. Hubby said I collect 2k from u. thanks." Approximately one hour later,

NJOKU responded "Ok." As another example, on or about February 20, 2017, NJOKU contacted NKONGHO via WhatsApp and stated: "Hello dear tell your hubby to please bring a big bag when he is coming to meet us." NKONGHO responded with the following: "Ok. He want to know which name u are using on ur passport so he can have his friend that work with custom to clear you gusy faster from the airport." In response, NJOKU messaged: "Eucharia. Njoku."

22. NJOKU's cellphone also contained a large number of emails and WhatsApp messages that NJOKU exchanged with brokers in China dealing with designer purses and shoes. On March 8, 2018, NJOKU communicates via WhatsApp with a subject using the phone number (310) 990-5118 (the subject is interested in buying high-end purses "Hermes Birkin"). NJOKU stated that the purses cost $850.00 each and then asked the subject what kind of leather she wants on the purse. Open source information indicates that these purses retail for between $7,000 and $30,000. The message is then followed by several pictures of Hermes purses. Law enforcement knows that individuals that deal in counterfeit commodities will often exchange photos of counterfeit commodities that will be bought and sold.

23. On or about October 4, 2018, NJOKU flew from Zurich, Switzerland on Swiss Air Flight 40 to Los Angeles International Airport, California. When NJOKU entered the United States, law enforcement interviewed NJOKU about her involvement in the Drunz Organization. During the interview, NJOKU admitted to knowing NKONGHO and UNAKALU. Law enforcement specifically asked NJOKU about iPhones and iPads that she received from a coconspirator, and NJOKU stated that she did not know what happened to "the stolen goods." At no time during the interview did law enforcement tell NJOKU that the iPhones and iPads had been stolen. As previously explained, the organization fraudulently obtained these Apple products from Company C using the above noted fraud scheme.

24. On or about September 12, 2018, a federal grand jury for the District of Maryland returned an indictment charging Peter UNKALAU, Khalid RAZAQ, Janet STURMER, Brandon ROSS, Saulina EADY, Saul EADY, Eunice NKONGHO, and Troy BARBOUR with various criminal violations, including Conspiracy to Commit Mail and Wire Fraud (18 U.S.C. § 1349), Money Laundering Conspiracy (18 U.S.C. § 1956(h)), Wire Fraud (18 U.S.C. § 1343), Mail Fraud (18 U.S.C. § 1341), Aggravated Identity Theft (18 U.S.C. § 1028A), Interstate Transportation of Stolen Property (18 U.S.C. § 2314), and/or Money Laundering (18 U.S.C. § 1956) (Crim. No. GJH-18-468).

25. On October 3, 2018, law enforcement arrested NKONGHO based on the federal arrest warrant from the indictment (Crim. No. GJH-18-468). Law enforcement advised NKONGHO of her *Miranda* rights; she then waived her rights orally and agreed to be interviewed by agents about her involvement in the conspiracy. During the interview, NKONGHO admitted that she had moved money for UNAKALU, which corroborated information that was found on the iPhone 7 found in possession of NKONGHO during a border search on or about March 20, 2017 when she returned to the United States (Miami, Florida) from travel to Havana, Cuba. Following this border search, on March 29, 2017, law enforcement obtained a federal search warrant from the District of Maryland, granting the examination of the device by law enforcement (Case Number TMD 17-0941). During the review of the cellphone, law enforcement discovered multiple conversations between NKONGHO and UNAKALU discussing the transfer of money between NKONGHO and Khalid RAZAQ for the payment and further facilitation of the fraud scheme. For example, on or about November 14, 2016, UNAKALU contacted NKONGHO and directed her to send RAZAQ $5,000 so that he can "ship product." During this conversation, UNAKALU sent RAZAQ a picture of the bank account information for RAZAQ and indicated that this bank was

where NKONGHO was to transfer the money. Shortly after, NKONGHO responded to UNAKALU by sending a picture of the bank confirmation showing the money has been transferred. These communications occurred over the WhatsApp messaging service.

26. On March 20, 2019, a federal grand jury for the District of Maryland returned an indictment against NJOKU, charging her with violations of 18 U.S.C. §§ 1349 (Conspiracy to Commit Mail Fraud and Wire Fraud), 1956(h) (Money Laundering Conspiracy), 1341 (Mail Fraud), and 2314 (Interstate Transportation of Stolen Property) (Crim. No. GJH 19-133). In addition, the U.S. District Court for the District of Maryland issued an arrest warrant. On or about March 25, 2019, law enforcement arrested NJOKU at the Los Angeles International Airport, California based on the federal arrest warrant.

C. There is Probable Cause to Believe That the Target Accounts Contain Relevant Evidence.

27. As detailed throughout this affidavit, I and other federal agents have recovered evidence revealing NJOKU and NKONGHO's extensive use of electronic devices in furtherance of the crimes under investigation, in particular, WhatsApp messages between the members of the conspiracy.

28. Based on the information uncovered to date in the investigation, there is probable cause to believe that NJOKU and NKONGHO used iPhones to send WhatsApp messages about the criminal activities they were involved in during the time period of January 1, 2016 through October 3, 2018. A federal search warrant was executed on NKONGHO's iPhone on or about March 29, 2017 (Case No. TMD 17-0941). NKONGHO's iPhone 7 was attached to Universal Forensic Extraction Device using software by Cellebrite; the extraction summary revealed that this cellphone's IMEI to be 359172072999638 and the existence of an Apple Account with the Apple

ID **euniqla@yahoo.com.** A federal search warrant was executed on NJOKU's iPhone on or about November 9, 2017 (Case No. TMD 17-3082). NJOKU's iPhone 7 was attached to Universal Forensic Extraction Device using software by Cellebrite; the extraction summary showed the cellphone's IMEI to be 355310083681787 and the existence of an Apple Account with the Apple ID **honeey178@aol.com**. The extraction of NJOKU's cellphone further revealed that the email addresses of **honeefashions@iCloud.com** and **GREATlove88@iCloud.com** were listed under her Apple Account in addition to **the honeefashions@iCloud.com** email address.

29. I understand from my training, knowledge, and experience, and the expertise of other law enforcement officers, that if an iPhone user has an AppleID and signs in with it on an iPhone, then the iPhone, by default, is set to back up data from the iPhone, unless the user changes the backup settings. This data is backed up to the iCloud linked to the AppleID. Consequently, I submit there is probable cause to believe that any iCloud data stored on the accounts with Apple ID's link to the IMEI and email addresses on the phones of NJOKU and NKONGHO contain additional fruits, instrumentalities, and evidence of the crimes described herein.

INFORMATION REGARDING APPLE ID AND iCLOUD[1]

30. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

---

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "iCloud: iCloud storage and backup overview," available at https://support.apple.com/kb/PH12519; and "iOS Security," available at http://images.apple.com/privacy/docs/iOS_Security_Guide.pdf.

31. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain

enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

32. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

33. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email

addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

34. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

35. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

36. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial

number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

37. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud.

38. I believe that evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records

described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

39. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

40. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

41. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan

to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

42. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators.

43. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

44. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B, pursuant to the procedure described in Section III of Attachment B.

19-1836TJS

CONCLUSION

45. Based on the forgoing, I request that the Court issue the proposed search warrant. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,

August Merker
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me on May 23, 2019

Honorable Timothy J. Sullivan
United States Magistrate Judge